Assurance LINCOLNSHIRE

For All Your Assurance Needs

Information Management Technology

Combined Assurance Status Report

Lincolnshire COUNTY COUNCIL

Working for a better future

January 2017

What we do best...

Innovative assurance services

Specialists at internal audit

Comprehensive risk management

Experts in countering fraud

...and what sets us apart

Unrivalled best value to our customers

Existing strong regional public sector partnership

Auditors with the knowledge and expertise to get the job done

Already working extensively with the not-for-profit and third sector

Combined Assurance Status Report

Assurance LINCOLNSHIRE
For All Your Assurance Needs

Contact details:

Simon Oliver
Chief Technology Officer

simon.oliver@lincolnshire.gov.uk

Combined Assurance Status Report

Assurance LINCOLNSHIRE
For All Your Assurance Needs

Introduction

This is the combined assurance report for Information Management Technology (IMT) within the Council.

By grouping the different sources of assurance in a single model we provide the basis for Senior Management and Audit Committees to gain a better understanding of their organisations assurance status and needs.

We do this by coordinating assurance arrangements – providing some structure – this is our Assurance Map.

We have well established Assurance Maps that help us to focus our work plans on the make or break risks that affect the successful delivery of services and strategic objectives. The Maps also recognise the importance of critical business systems that support successful delivery and 'protect the business' – the due diligence activities.

The Maps give an overview of assurance provided across the whole organisation – not just those from Internal Audit – making it possible to identify where assurances are present, their source, and where there are potential assurance 'unknowns or gaps'.

The Maps are an invaluable tool for senior managers, providing a snapshot of assurance at any point of time. This report explores those assurances in more detail.

We gathered and analysed assurance information in a control environment that:

- takes what we have been told on trust, and
- encourages accountability with those responsible for managing the service.

Scope

We gathered information on our:

- **Critical systems** – those areas identified by senior management as having a significant impact on the successful delivery of our priorities or whose failure could result in significant damage to our reputation, financial loss or impact on people.
- **Due diligence activities** – those that support the running of the Council and ensure compliance with policies.
- **Key risks** – found on our strategic risk register, operational risk registers or associated with major new business strategy / change.
- **Key projects** –supporting corporate priorities / activities.
- **Key partnerships** – partnerships that play a key role in successful delivery of services

Methodology

To ensure our combined assurance model shows assurances across the entire Council, not just those from Internal Audit, we leverage assurance information from your 'business as usual' operations. Using the '3 lines of assurance' concept:

Our approach includes a critical review or assessment on the level of confidence the Board can have on its service delivery arrangements, management of risks, operation of controls and performance.

We did this by:

- Speaking to senior and operational managers who have the day to day responsibility for managing and controlling their service activities.
- Working with corporate functions and using other third party inspections to provide information on performance, successful delivery and organisational learning.
- Using the outcome of Internal Audit work to provide independent insight and assurance opinions.
- Considering other information and business intelligence that feed into and has potential to impact on assurance.

We used a Red (low), Amber (medium) and Green (high) rating to help us assess the level of assurance confidence in place.

The overall assurance opinion is based on the assessment and judgement of senior management. Internal audit has helped co-ordinate these and provided some challenge **but** as accountability rests with the Senior Manager we used their overall assurance opinion.

Key Messages

Whilst the Council continues to benefit from a professional, experienced and capable internal IT Governance and Assurance function, those aspects which rely on our IT Service Provider continue to fall short of expectation.

Information Security continues to improve and the Management Rating shows all aspects to be either green, or trending to green. The IMT team has continued to develop and improve the Council's approach to Information Governance and has established a sound and robust framework designed to support the way LCC handles information, in particular, the personal and sensitive data relating to our customers and employees.

The development and implementation of a formal information security management system (ISMS) which has been independently certified against a recognised international standard (ISO 27001:13) was achieved in November 2016 in partnership with Serco. This assists in improving the overall security posture by managing risk more effectively and will continue to develop over time.

Work continues to improve policies and procedures to support secure working practices and we have improved the way the Council reacts to security incidents. We have also been subject of audit from the Information Commissioners Office (ICO) with a positive outcome.

We are looking to embrace new technology designed to help protect against external threats, following two malware outages, and to provide tools to staff that ensure they are able to work safely and within the policy framework. The delivery issues with the IT Service Provider are hampering the introduction of these initiatives.

The management of IT Contracts and Financial aspects remains in a very good position with a good level of assurance continuing to being evidenced. The management of cost savings through contract review, and the monitoring of 3rd party contracts remain robust.

Poor performance by the IT Service Provider has hampered improvements, or in some aspects worsened, the Council's ability to provide the levels of Service Delivery contracted for. The IT Service Provider continues to offer a reactive, rather than proactive service, which causes an increased risk of system outages and impact on Council service area delivery.

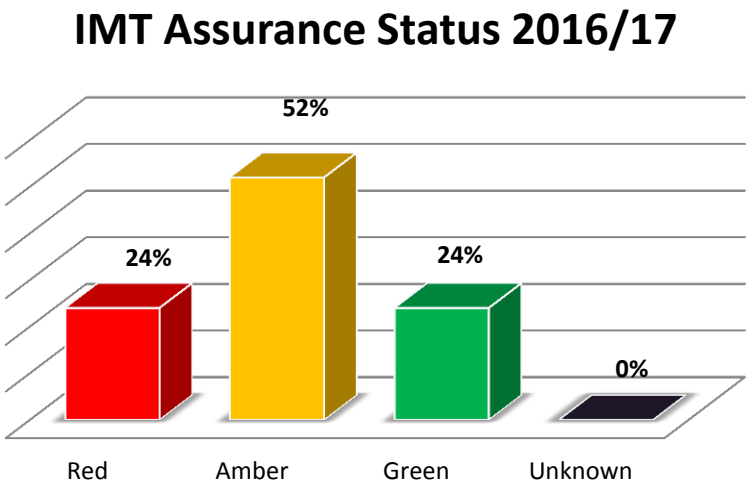
Maturity assessments undertaken during 2016 in regards to the breadth of 'day to day' services have demonstrated that the IT Service Provider is not fulfilling the contractual commitments in many areas. The continued difficulties in introducing Service Improvement Plans (SIPS) to rectify service deficiencies are an area of considerable frustration and there is little evidence that this will be resolved in the near future.

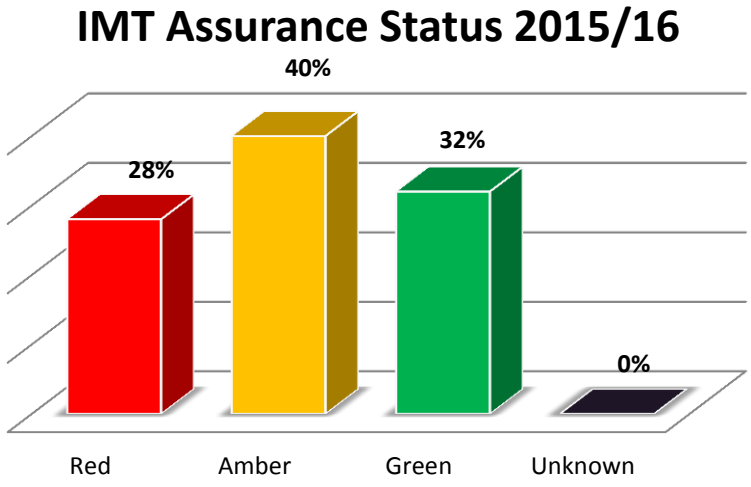
Combined Assurance Status Report

IMT Project Delivery remains a significant risk to the Council. The delivery (and the monitoring of delivery) of projects commissioned with the IT Service Provider is falling short of the most basic requirements of the Council. This is reflected in the failure to deliver the IMT_KPI_11 measurement (assessing the performance of project delivery) to date. This is having a significant impact on the Council as we are unable to deliver the level of innovation required and is preventing Service Areas to deliver their own improvement plans and technology enabled efficiencies. Effectively, IT delivery is having a negative impact on the Council's ability to meet the changing need of the Organisation.

Corporate Projects, which are commissioned without considering the ICT implications at the start, are causing some technical and resourcing issues, but are being managed where possible.

The previous ICT Assurance Map process identified that the situation with the IT Service Provider had, and continues to, place excessive workloads onto key staff to manage the service. Retaining key staff and maintaining the current commitment to resolve the issues with the IT Service Provider is a risk that is continuing to worsen.





Combined Assurance Status Report

Assurance LINCOLNSHIRE
For All Your Assurance Needs

IMT ASSURANCE MAP	RAG Rating
ICT Governance	
Financial Management for IT Services	G
External IMT Governance (Projects and Strategy)	A
Service Reviews and Improvement Plans	R
ICT Projects	
IT Strategy Management	A
IMT-Led Projects Governance	R
Information Security	
Information Governance	A
Records Management	A
Corporate Policy and Procedures	G
Service Design	
Service Catalogue management	A
Service-level management	G
Availability management	A
Capacity management	R

IMT ASSURANCE MAP	RAG Rating
IT service continuity management / DR	R
Information security management system	A
Supplier Management	G
Service Transition	
Technical Change Management	G
Service asset and configuration management	R
Service Operation	
Service desk	G
Application management	A
IT operations management	A
Technical management	A
Incident management	A
Request fulfilment	A
Problem management	R
Identity management	A

Key Risks

Strategic Risks

Council's highest rated Strategic Risk for this area of the business

Cyber Security

Cyber Security risks arise from a broad spectrum of internal and external threats which seek to negatively impact the confidentiality, integrity or availability of an information system and/or the information residing therein.

The Council and Serco have achieved formal independent certification to ISO 27001:13, an international standard that describes best practice for an information security management system (ISMS). The scope of certification includes IMT services to a cyber-attack. While we will never be immune from cyber-attacks, successfully implementing ISO 27001:13 is evidence that we have achieved a solid base on which to continually improve cyber-attack is better understood.

The lack of maturity of a number of key controls, alongside gaps identified as part of the ISMS implementation, does not yet give us enough confidence to reduce the current risk score, therefore effort will continue to focus on:

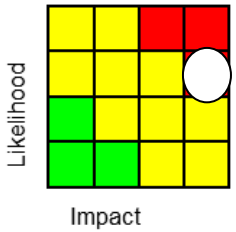
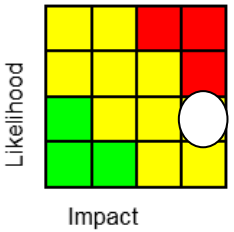
- Asset Management
- User Access Management
- Operational Procedures and responsibilities
- Protection from Malware
- Technical Vulnerability Management
- Network Security Management
- Supplier Relationships
- Incident Management
- Monitoring

Operational Risks

The IMT operational risks are:

1. Inability to deliver IT transformational change
2. Lack of capacity within IMT function to deliver the priority projects
3. Infrastructure failure due to a lack of resilience (Business Continuity/Disaster Recovery) and Cyber Attack
4. Continued high levels of Data Breaches
5. Lack of appropriate IT/IG provided to key Council Strategic Projects
6. Continued poor delivery from the IT Service provider

Strategic Risk Register as at January 2017

Risk Owner	Risk description	Risk Appetite (How much risk are we prepared to take & the total impact of risk we are prepared to accept)	Current risk score	Target risk score	Assurance Status (Full, Substantial, Limited, No)	Assurance - Direction of Travel (Improving, Static, Declining)
Richard Wills	**Cyber Security**	**Cautious**			Limited	Improving